

AMENDMENTS TO THE SPECIFICATION:

Please replace the following identified paragraphs with the text below:

[0002] [[1.]] In recent years e-mail has become an indispensable business tool. E-mail has replaced "snail mail" for many business practices because it is faster, cheaper and generally more reliable. But there remain some mail applications where hard copy is still dominant, such as registered and certified mail. For example, when a letter is sent by certified mail the sender is provided with a receipt to prove that the letter was mailed. A returned registered mail receipt adds the Postal Service's confirmation that the letter was successfully delivered to the addressee or the addressee's authorized agent. Additionally, private couriers such as Federal Express® and United Parcel Service® (UPS) provide some type of delivery confirmation. Since every piece of courier mail is, in effect, registered, it is natural for consumers to turn to these services when they want proof of delivery.

[000324] [[7.]] At the sender's mail client or mail transport agent: before the message is transmitted, the system assigns the message an alphanumeric identification tag that uniquely individualizes the message within the system. The system also enumerates the addressees of the message so as to create a unique alphanumeric identifier for each recipient of the message.

[000325] [[8.]] The identifiers are stored in a database together with the email address of the sender of the message and the email addresses of the intended recipients of the message.

[000326] [[9.]] The system provides for the message to be in MIME multi-part format in accordance with RFC 2045 and RFC 2046 and for the primary body text to be in HTML format.

[000327] [[10.]] For each copy of the message delivered to each destination the system includes an HTML "MAILTO" link in the message together with an invitation to click on the link if the recipient wishes to receive proof of transmission or delivery of the reply. The address included in the MAILTO link is a fictitious address at a domain controlled by the sender or the sender's agent. The address is formed from the message and destination IDs. Thus if the message ID was "ABC123", then, for a copy of the message to be delivered to a destination "2" of the message, the link might appear as

- [000331] [[11.]] The message is then transmitted.
- [000332] [[12.]] When a recipient of the message, using an HTML enabled mail browser, clicks on the link, the browser will open the recipient's default mail client with a message already addressed to the embedded address. The recipient composes a reply and sends it to the fictitious address.
- [000333] [[13.]] The message arrives at the RPost server.
- [000334] [[14.]] On receiving the message the RPost Server parses the destination address of the reply to extract the message and destination ID. The server queries the database to recover the true address of the original sender of the message.
- [000336] Upon opening of the message (1303) (1308), the recipient's client program executes an HTTP call to a Web Server (1309). On receiving the HTTP call (1311) the HTTP Server extracts information from the HTTP header including the IP address of the recipient's client (1310), and the message (1311) and recipient ID included in the HTTP call (1312). The Server consults the database to identify the sender and recipient of the message (1313) and a notice of the opening of the message is transmitted to the sender of the message (1314).